



Stored XSS through list fields on Cargo's page values and Special:CargoTables

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-39841
State	PUBLISHED
Assigner	wikimedia-foundation
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 20:16:34 UTC
Updated	2026-04-08 21:27:00 UTC
Description	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in Wikimedia Foundation Medi

Risk And Classification

Primary CVSS: v4.0 6.3 MEDIUM from c4f26cc8-17ff-4c99-b5e2-38fc1793eacc

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:H/SI:H/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000470000 probability, percentile 0.144940000 (date 2026-04-09)

Problem Types: CWE-80 | CWE-80 CWE-80 Improper neutralization of Script-Related HTML tags in a web page (basic XSS)

Version	Source	Type	Score	Severity	Vector
4.0	c4f26cc8-17ff-4c99-b5e2-38fc1793eacc	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Passive

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:N/SC:H/SI:H/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Wikimedia Foundation	Mediawiki - Cargo Extension	affected 3.8.7 custom	Not specified

References

Reference	Source	Link	Tags
phabricator.wikimedia.org/T416389	c4f26cc8-17ff-4c99-b5e2-38fc1793eacc	phabricator.wikimedia.org	
gerrit.wikimedia.org/r/c/mediawiki/extensions/Cargo/+/1237973	c4f26cc8-17ff-4c99-b5e2-38fc1793eacc	gerrit.wikimedia.org	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

Vendor Comments And Credit

Discovery Credit
CNA: Alex44019 (en)

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report